

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-208406

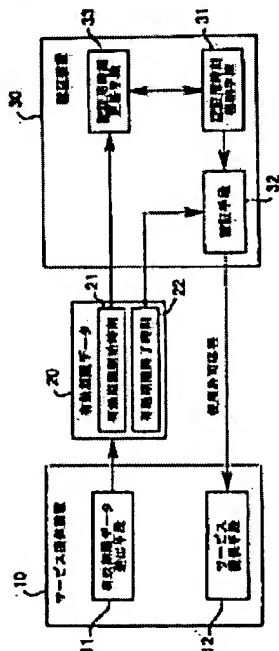
(43)Date of publication of application : 25.07.2003

(51)Int.Cl. G06F 15/00  
H04L 9/32

(21)Application number : 2002-334052 (71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 14.07.1997 (72)Inventor : KONO KENJI  
TAGUCHI MASAHIRO  
CHIBA KENJI

(54) SERVICE PROVIDING SYSTEM, AUTHENTICATION DEVICE, AND  
COMPUTER-READABLE RECORDING MEDIUM RECORDING AUTHENTICATION  
PROGRAM



(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal use by fabricating a set time of a service providing device in providing the online service with an appointed period.

SOLUTION: An effective time limit data sending means 11 of a service providing device 10 sends the effective time limit data 20 corresponding to a specific service to an authentication device 30. The authentication device 30 sends a use permission response to the service providing device 10 by an authentication means 32 when the authentication time is before the effective time limit termination time. An effective time limit starting time 21 is stored in an authentication time storing means 31 as a new

authentication time in a case when the authentication time is before the effective time limit starting time 21. A service providing means 12 of the service providing device 10 provides the service to the user only when it receives the user permission response.

Japanese Laid-Open Patent Publication No.2003-208406 published on July 25, 2003. (partial English Translation)

**【0051】**

[S8] A decryption key decrypting part 203 decrypts an encrypted decryption key 315 by use of secret information 252 stored in PROM 250, and sends it back to the PC 110.

[S9] After receiving the decryption key, the PC 110 decrypts an encrypted software 320 on the basis of a command from a capsule activating program 311, and executes the software. At this time, the software 320 is not completely decrypted, instead, only one part to be executed is decrypted so as to be developed in the volatile memory. And then, the software decrypted and developed in the volatile memory is set to be deleted after the software is finished. Accordingly, there is no risk that the decrypted data is illegally used.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-208406

(P2003-208406A)

(43) 公開日 平成15年7月25日 (2003.7.25)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D	5 B 0 8 5
			3 3 0 B	5 J 1 0 4
			3 3 0 G	
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D	
			6 7 5 Z	
審査請求 有 請求項の数 9 O L (全 16 頁)				

(21) 出願番号 特願2002-334052(P2002-334052)  
(62) 分割の表示 特願平9-188246の分割  
(22) 出願日 平成9年7月14日(1997.7.14)

(71) 出願人 000005496  
富士ゼロックス株式会社  
東京都港区赤坂二丁目17番22号  
(72) 発明者 河野 健二  
神奈川県足柄上郡中井町境430 グリーン  
テクなかい 富士ゼロックス株式会社内  
(72) 発明者 田口 正弘  
神奈川県足柄上郡中井町境430 グリーン  
テクなかい 富士ゼロックス株式会社内  
(74) 代理人 100092152  
弁理士 服部 毅巖

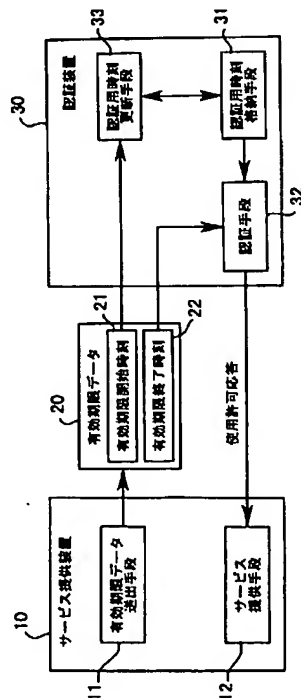
最終頁に続く

(54) 【発明の名称】 サービス提供システム、認証装置及び認証プログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止できるようにする。

【解決手段】 サービス提供装置10の有効期限データ送出手段11が、特定のサービスに対応する有効期限データ20を認証装置30へ送出する。認証装置30では、認証用時刻が有効期限終了時刻より前の時刻である場合には、認証手段32により、使用許可応答がサービス提供装置10へ送られる。また、認証用時刻が有効期限開始時刻21より前の時刻である場合には、認証用時刻更新手段33により、有効期限開始時刻21が新たな認証用時刻として認証用時刻格納手段31に格納される。サービス提供装置10のサービス提供手段12は、使用許可応答を受け取った場合にのみ、ユーザに対してサービスを提供する。



## 【特許請求の範囲】

【請求項 1】 サービス提供装置と認証装置とから構成されるサービス提供システムであって、前記サービス提供装置は、特定のサービスに対応して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データを前記認証装置に出力する有効期限データ送出手段と、前記認証装置から返された使用許可応答に基づいて前記特定のサービスを提供するサービス提供手段と、を具備しており、前記認証装置は、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から受け取った前記有効期限データに含まれる前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を具備していることを特徴とするサービス提供システム。

【請求項 2】 サービス提供装置と認証装置とから構成されるサービス提供システムであって、前記サービス提供装置は、特定のサービスに対応して設定された有効期限開始時刻と有効期限終了時刻と該有効期限開始時刻および該有効期限終了時刻に対する署名とからなる有効期限データを前記認証装置に出力する有効期限データ送出手段と、前記認証装置から返された使用許可応答に基づいて前記特定のサービスを提供するサービス提供手段と、を具備しており、前記認証装置は、認証用時刻を保持する認証用時刻格納手段と、前記サービス提供装置から受け取った前記有効期限データに含まれる前記署名に基づいて前記有効期限終了時刻が正しいことを確認した上で前記認証用時刻が前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を具備していることを特徴とするサービス提供システム。

【請求項 3】 サービス提供装置と認証装置とから構成されるサービス提供システムであって、前記サービス提供装置は、暗号化された特定のサービスに対応して設定された有効

期限開始時刻、有効期限終了時刻、および該サービスの復号鍵が暗号化されたデータからなる認証データを前記認証装置に出力する認証データ送出手段と、前記認証装置から返された前記復号鍵を含む使用許可応答に基づいて前記サービスを復号して提供することを可能とするサービス提供手段と、を具備しており、前記認証装置は、認証用時刻を保持する認証用時刻格納手段と、前記暗号化された復号鍵を復号する秘密情報を保持する秘密情報格納手段と、前記認証用時刻が前記サービス提供装置から受け取った前記認証データに含まれる前記有効期限終了時刻より前の時刻である場合、前記秘密情報で前記復号鍵を復号し、復号された該復号鍵を含む前記使用許可応答を前記サービス提供装置に対して出力する認証手段と、前記認証用時刻が前記認証データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を具備していることを特徴とするサービス提供システム。

【請求項 4】 サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データに基づいて該サービスの使用権の認証を行う認証装置であって、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を有することを特徴とする認証装置。

【請求項 5】 サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と、該有効期限開始時刻および該有効期限終了時刻に対する署名とからなる有効期限データに基づいて該サービスの使用権の認証を行う認証装置であって、認証用時刻を保持する認証用時刻格納手段と、前記サービス提供装置から出力された前記有効期限データに含まれる前記署名に基づいて前記有効期限終了時刻が正しいことを確認した上で前記認証用時刻が前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻

刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、  
を有することを特徴とする認証装置。

【請求項 6】 サービス提供装置から出力される暗号化された特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と該暗号化されたサービスの復号鍵が暗号化されたデータとからなる認証データに基づいて該サービスの使用権の認証を行う認証装置であって、

認証用時刻を保持する認証用時刻格納手段と、  
前記暗号化された復号鍵を復号する秘密情報を保持する秘密情報格納手段と、

前記認証用時刻が前記サービス提供装置から出力された前記認証データに含まれる前記有効期限終了時刻より前の時刻である場合、前記秘密情報で前記復号鍵を復号し、復号された該復号鍵を含む前記使用許可応答を前記サービス提供装置に対して出力する認証手段と、  
前記認証用時刻が前記認証データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、  
を有することを特徴とする認証装置。

【請求項 7】 サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

認証用時刻を保持する認証用時刻格納手段と、  
前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、  
前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に変更する認証用時刻更新手段と、

してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 8】 サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と該有効期限開始時刻および該有効期限終了時刻に対する署名からなる有効期限データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

認証用時刻を保持する認証用時刻格納手段と、  
前記サービス提供装置から出力された前記有効期限データに含まれる前記署名に基づいて前記有効期限終了時刻が正しいことを確認した上で前記認証用時刻が前記有効

期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、

前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、

してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 9】 サービス提供装置から出力される暗号化された特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻と該暗号化されたサービスの復号鍵が暗号化されたデータとからなる認証データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

認証用時刻を保持する認証用時刻格納手段と、  
前記暗号化された復号鍵を復号する秘密情報を保持する秘密情報格納手段と、

前記認証用時刻が前記サービス提供装置から出力された前記認証データに含まれる前記有効期限終了時刻より前の時刻である場合、前記秘密情報で前記復号鍵を復号し、復号された該復号鍵を含む前記使用許可応答を前記サービス提供装置に対して出力する認証手段と、  
前記認証用時刻が前記認証データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、

してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はサービス提供システム、認証装置及び認証プログラムを記録したコンピュータ読み取り可能な媒体に関し、特に使用権の有効性を確認してサービスを提供するサービス提供システム、サービスの使用権の認証を行う認証装置及びサービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な媒体に関する。

【0002】

【従来の技術】 近年のネットワークの発達によってデジタル社会が到来し、欧米を中心とした電子商取引や電子マネーの運用が開始された今日、IC(Integrated Circuit)カードは、電子マネーを格納する電子財布などのさまざまなサービスを受けるための個人認証装置として重要な役割を担うようになっている。このような中で IC カードは、データを記憶するだけの単なるメモリーカードという位置づけから、CPU(Central Processing Unit)を搭載しメモリに対するアクセス制限機能を有す

るようになり、さらに今日では高度な暗号演算機能を有し、ユーザ認証を行うものも登場している。

【0003】ただし、ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) 7816 準拠の IC カードには厚さの制限があるため、電源を内部に持つことができないという制約がある。また、製造コストの観点から、IC カード内に電源を持たせるのは有効ではない。このため IC カードの電源およびクロックは接続装置(interface device)により供給され、電源の供給が断たれると IC カード内部で時計機能を働かせておくことはできない。従って、IC カードに時刻を書き込む必要があるときには、信頼できる端末でのみ時刻の更新ができるようにしていた。

【0004】

【発明が解決しようとする課題】ところで、今後の IC カードを用いた認証を行うシステムの利用形態を考えると、利便性や通信コストの観点からローカルな環境やオフラインでの利用が必要とされる。このような環境において、例えば、ソフトウェアのライセンス管理を IC カードで行おうとすると、時間や期間によるアクセス管理を行う必要がある。その場合、時刻に関するデータを IC カードで管理しなければならない。

【0005】しかし、ローカルな環境では、時間の管理をユーザの管理下にある PC(Personal Computer) により行わなければならない、ユーザの管理下にある PC では、いくらでもユーザによる時間の詐称が可能である。また、UNIX(登録商標)のクライアント・サーバシステムにおいては、時刻サーバを設けて、定期的にクライアントのマシンから時刻の同期を取る方法がある(下山智明他/SUNシステム管理/アスキー出版/p. 249(1991))が、このような管理は、クライアントとサーバが常に接続されていることが前提となり、またクライアントから同期要求を出すのでクライアントでの詐称は依然として容易であることに変わりはない。従って、IC カードを用いた時間や期間によるライセンス管理が正常に機能し難いという問題点があった。

【0006】なお、ネットワークを介したオンラインの利用制限が可能であれば、IC カードの方で利用期間を管理する必要はなくなるが、今後のサービスの多様性を考慮すると、非現実的である。例えば、利用期限のあるサービスをユーザのローカルなコンピュータ等で実現するような場合、サービスを提供するソフトウェア等はオンラインで利用するよりもオフラインで利用した方がユーザには利便性があり、しかも経済的である。

【0007】また、サービス提供者(プロバイダ)の方でも、ユーザの管理をサービスが利用される度に個別にオンラインで行うには、複雑な管理と非常に巨大なデータベースが必要となり、過大な設備投資が強いられる。従って、利便性や経済性を考慮すると、サービスの有効

期間管理がオフラインで行えることが不可欠である。

【0008】本発明はこのような問題に鑑みてなされたものであり、期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止できるサービス提供システムを提供することを目的とする。

【0009】また、本発明の他の目的は、期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止できる認証装置を提供することである。

【0010】さらに、本発明の別の目的は、期間を指定したオフラインでのサービス提供の際に、サービス提供装置の設定時刻の詐称による不正使用を防止した認証処理をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することである。

【0011】

【課題を解決するための手段】本発明では上記課題を解決するために、サービス提供装置と認証装置とから構成されるサービス提供システムであって、前記サービス提供装置は、特定のサービスに対応して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データを前記認証装置に出力する有効期限データ送出手段と、前記認証装置から返された使用許可応答に基づいて前記特定のサービスを提供するサービス提供手段と、を具備しており、前記認証装置は、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から受け取った前記有効期限データに含まれる前記有効期限終了時刻より前の時刻である場合、前記サービス提供装置に対して前記使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を具備していることを特徴とするサービス提供システムが提供される。

【0012】このサービス提供システムによれば、特定のサービスの提供を望むユーザは、サービス提供装置の有効期限データ送出手段を用いて、有効期限データを出力する。すると、認証用時刻が前記有効期限終了時刻より前の時刻である場合、認証装置内の認証手段により、サービス提供装置に対して使用許可応答が出力される。また、認証用時刻が有効期限データに含まれる有効期限開始時刻より前の時刻である場合、認証用時刻更新手段により、認証用時刻が有効期限開始時刻で示された時刻に更新される。一方、認証手段からの使用許可応答が出力されると、サービス提供手段による、ユーザへのサービスの提供が可能となる。

【0013】また、本発明では上記課題を解決するために、サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻

とからなる有効期限データに基づいて該サービスの使用権の認証を行う認証装置であって、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に更新する認証用時刻更新手段と、を有することを特徴とする認証装置が提供される。

【0014】この認証装置によれば、サービス提供装置から有効期限データが送られると、認証用時刻が前記有効期限終了時刻より前の時刻である場合、認証装置内の認証手段により、サービス提供装置に対して使用許可応答が出力される。また、認証用時刻が有効期限データに含まれる有効期限開始時刻より前の時刻である場合、認証用時刻更新手段により、認証用時刻が有効期限開始時刻で示された時刻に更新される。

【0015】また、本発明では上記課題を解決するために、サービス提供装置から出力される特定のサービスに対して設定された有効期限開始時刻と有効期限終了時刻とからなる有効期限データに基づいて該サービスの使用権の認証をコンピュータに行わせるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に変更する認証用時刻更新手段と、してコンピュータを機能させるための認証プログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【0016】この認証プログラムを記録した媒体に格納されたプログラムをコンピュータで実行すれば、認証用時刻を保持する認証用時刻格納手段と、前記認証用時刻が前記サービス提供装置から出力された前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記サービス提供装置に対して前記サービスの使用許可応答を出力する認証手段と、および前記認証用時刻が前記有効期限データに含まれる前記有効期限開始時刻より前の時刻である場合、前記認証用時刻を前記有効期限開始時刻で示された時刻に変更する認証用時刻更新手段の各機能がコンピュータによって実現される。

【0017】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は、本発明の原理構成図であ

る。本発明のサービス提供システムは、ユーザに各種サービスを提供するサービス提供装置10と、サービス提供装置10の提供するサービスの使用権の有効性を認証する認証装置30とで構成される。

【0018】サービス提供装置10において、有効期限データ送出手段11は、特定のサービスに対応して設定された有効期限開始時刻21と有効期限終了時刻22とからなる有効期限データ20を、認証装置30へ出力する。サービス提供手段12は、使用許可応答が入力された場合にのみ、特定のサービスの提供を可能とする。

【0019】認証装置30において、認証用時刻格納手段31は、認証用時刻を保持する。認証手段32は、サービス提供装置10から有効期限データ20を受け取ると、認証用時刻格納手段31に格納されている認証用時刻と有効期限終了時刻22とを比較し、認証用時刻が有効期限終了時刻22より前の時刻である場合、サービス提供装置10に対して使用許可応答を出力する。認証用時刻更新手段33は、サービス提供装置10から有効期限データ20を受け取ると、認証用時刻格納手段31に格納されている認証用時刻と有効期限開始時刻21とを比較し、認証用時刻格納手段31に格納されている認証用時刻が有効期限開始時刻21より前の時刻である場合には、有効期限開始時刻21を新たな認証用時刻として認証用時刻格納手段31に格納する。

【0020】このようなサービス提供システムによれば、サービスの提供者側は、各サービスに対応して有効期限データ20を設定する。そして、特定のサービスの提供を受けようとするユーザは、サービス提供装置10の有効期限データ送出手段11により、特定のサービスに対応する有効期限データ20を認証装置30へ送出する。

【0021】有効期限データ20を受け取った認証装置30では、認証手段32により、認証用時刻格納手段31内の認証用時刻と有効期限終了時刻とが比較され、認証用時刻が有効期限終了時刻より前の時刻である場合には、使用許可応答がサービス提供装置10へ送られる。また、認証用時刻更新手段33により、認証用時刻と有効期限開始時刻21とが比較され、認証用時刻が有効期限開始時刻21より前の時刻である場合には、有効期限開始時刻21が新たな認証用時刻として認証用時刻格納手段31に格納される。

【0022】サービス提供装置10のサービス提供手段12は、使用許可応答を受け取った場合にのみ、ユーザに対してサービスを提供する。ここで、使用許可応答とは、サービス提供装置10の入力データに対する認証装置30の署名であったり、サービスを利用するために必要な情報であったりする。また、使用許可応答を送信する場合は、リプレイアタック等に対応するために、乱数を用いた秘密通信を用いてもよい。

【0023】このようにして、サービス提供装置がオフ

ラインの状態でも、有効期限を指定したサービスの使用権の管理を行うことができる。しかも、認証用時刻は、サービスの提供を受ける際に有効期限開始時刻に更新され、その時刻を過去の時刻へ戻すことはできないため、ユーザが認証用時刻を詐称することはできない。

【0024】本発明のサービス提供装置を用いて、ユーザはさまざまなサービスの提供を受けることができる。例えばそれは従来技術でも述べたように、ソフトウェアの使用権であったり、電子マネー等の有価情報であったり、さらには他のサービスを使用するためのチケットの

ようなものであったりする。  
【0025】次に、本発明の具体的な第1の実施の形態について、プロバイダが提供するソフトウェアのライセンス管理をICカードで行う場合を例にとりて説明する。図2は、ICカードを用いた認証システムの概略構成を示す図である。ユーザが使用するパーソナルコンピュータ(PC)110は、インターネットなどのネットワーク120を介してセンタ130と繋がっている。センタ130では、ユーザの登録および、ユーザデータやユーザに提供したサービスの履歴等の管理が行われる。そして、センタ130は、PC110からの要求に応じて、カプセル化されたソフトウェア(以下、単に「カプセル」という)300を提供する。ここでいうカプセル化とは、例えばDES(Data Encryption Standard)等の暗号アルゴリズムを用いて暗号化し、そのままでは使用できないようにすることを指す。

【0026】また、PC110には、RS-232C \ (アメリカ電子工業会によって規定されたデータ通信用インタフェース)などのインタフェースにより、リーダ/ライタ140が接続されている。ユーザは、このリーダ/ライタ140にICカード200を接続することで、センタ130から取得したソフトウェアの使用権に関する認証を行うことができる。

【0027】ICカード200は、ソフトウェアを提供するプロバイダ若しくはプロバイダの依頼を受けたセンタ130からユーザに渡されるものである。なお、この例では、PC110によってサービスを利用するものとしているが、サービスを利用するためのローカルな端末装置はPCには限定されず、例えばワークステーションであったり、サーバであったり、ATM(Auto Teller Machine) 端末であったりする。

【0028】図3は、カプセルの例を示す図である。カプセル300は、ヘッダ部310と暗号化されたソフトウェア320とで構成される。ヘッダ部310はカプセルの起動を行うためのカプセル起動プログラム311と、ICカードが認証ステップを行うために必要な認証データとに分けられる。

【0029】カプセル起動プログラム311は、認証データ送出処理、ユーザ情報取得処理、ソフトウェア復号処理及びソフトウェア実行処理の各処理を、PC110

に実行させるためのプログラムである。認証データ送出処理とは、カプセル300内のヘッダ部310に含まれた認証データをICカード200へ送信する処理である。ユーザ情報取得処理とは、ユーザに対して、ユーザのID(ユーザ固有の識別情報)やパスワードの入力を促し、入力されたID等をICカード200に送信する処理である。ソフトウェア復号処理とは、ICカード200から復号鍵を受け取り、その復号鍵を用いて暗号化されたソフトウェア320を復号する処理である。ソフトウェア実行処理とは、復号されたソフトウェアを実行する処理である。

【0030】また、ヘッダ部310内の認証データは、ソフトウェア認証データ312、ソフトウェア使用権認証データ313、有効期限認証データ314、及び暗号化された復号鍵315で構成される。ソフトウェア認証データ312には、例えば、ソフトウェアの識別子(ID)やプロバイダの署名が含まれる。ソフトウェア使用権認証データ313には、ユーザ認証が成功した際に、そのユーザに対応する使用権を認証するための情報が格納されている。有効期限認証データ314は、暗号化されたソフトウェア320の有効期限を示すデータである。暗号化された復号鍵315は、カプセル300を復号するための復号鍵であり、この復号鍵を復号するための秘密情報(復号鍵)は、ICカード200内に予め格納されている。

【0031】図4は、有効期限認証データ314の構造を示す図である。図のように、有効期限認証データ314には、有効期限開始時刻314a、有効期限終了時刻314b及びセンタの署名314cが含まれている。ここでセンタの署名314cとは、例えば有効期限開始時刻314aと有効期限終了時刻314bをセンタの署名鍵で署名したものである。このセンタの署名314cは、有効期限開始時刻314aと有効期限終了時刻314bが詐称されていないことが確認できる機構が他に存在すれば必ずしも必要ではない。

【0032】図5は、ICカードのハードウェア構成を示す図である。ICカード200は、CPU210を中心として、1つのコンピュータシステムが構築されている。CPU210には、内部のシステムバスを介して他の各種要素が接続されている。RAM(Random Access Memory)220は、CPU210が処理すべきデータを一時的に格納する。ROM(Read Only Memory)230は、ICカード200に必要な機能をCPU210に実行させるための認証プログラムが格納されている。入出力装置(I/O)240は、所定の規格に従って、リーダ/ライタ140との間でデータ通信を行う。PROM(Programmable Read Only Memory)250は、有効期限の認証に用いられるICカード時刻や、暗号化された復号鍵315を復号するための秘密情報などが格納されている。



【0033】このようなハードウェア構成のICカード200によって、以下のような処理機能が実現されている。図6は、ICカードの処理機能を示すブロック図である。認証部201は、PC110から送られた認証データの内容に基づいて、カプセル300の使用を認めるか否かの判断を行う。具体的には、使用を認める場合にはカプセル300の使用を許可する旨の判定を行い、使用を認めない場合には、「エラー」の情報をPC110に返す。認証部は、以下のような目的別の認証部を有している。

【0034】ソフトウェア認証部201aは、ソフトウェア認証データ312を参照し、カプセル300が正当なプロバイダにより提供されたものかどうかを認証する。これによりコンピュータウイルス等の侵入を防ぐことができる。

【0035】ユーザ認証部201bは、PC110から送られたユーザのIDやパスワードに基づいて、そのユーザがICカード200の所有者であることを認証する。ソフトウェア使用権認証部201cは、ソフトウェア使用権認証データ313に基づいて、このICカード200の所有者が、カプセル300内のソフトウェアを使用する権利を有していることを認証する。例えば、カプセル300内のソフトウェアがある一定以上の役職の者しか使用できない場合、このICカード200の所有者の役職を表す値が所定の値以下であれば、使用不可と判定する。

【0036】有効期限認証部201dは、有効期限認証データ314の有効期限終了時刻314bとICカード時刻251とを照らし合わせ、ICカード時刻251が有効期限終了時刻314b以前であることを認証する。

【0037】以上の各認証部によりカプセル300の使用が許可されると、その情報がICカード時刻更新部202と復号鍵復号部203とに送られる。ICカード時刻更新部202は、カプセル300の使用が許可された際に、有効期限認証データ314の中の有効期限開始時刻314aとICカード時刻251とを比較する。そして、有効期限開始時刻の方が大きい場合には、ICカード時刻251を有効期限開始時刻に書き換える。

【0038】復号鍵復号部203は、PROM250に格納されている秘密情報252を用いて、暗号化された復号鍵315を復号する。そして、復号された復号鍵を、PC110に転送する。

【0039】以上のような構成のシステムにおいて、まず、プロバイダにより作成されたソフトウェアは、センタ130またはそれに準ずる機関によりカプセル化され、カプセル300が生成される。

【0040】次に、ユーザはネットワーク120またはCDROM等によりカプセル300を入手する。そして、ユーザは、自己の所持するICカード200をリーダ/ライタ140に接続し、入手したカプセル300を

PC110で起動する。

【0041】PC110は、カプセル300の起動命令を受けると、カプセル起動プログラム311を読み込み、その命令にしたがってICカード200と通信し、ICカード200に認証データを渡す。すると、ICカード200が認証ステップを実行することで認証が行われる。正しく認証されればソフトウェアを復号するための復号鍵がICカード200からPC110に送られる。PC110は、受け取った復号鍵で暗号化されたソフトウェア320を復号し、平文となったソフトウェアを実行する。

【0042】なお、カプセル起動プログラム311とICカード200と間の通信はICカードのセキュアメッセージング機能を用いることで復号鍵等が露呈することを防ぐことが出来る。また、ソフトウェアが復号された後もカプセル起動プログラムを経由しなければ実行できないようにすることで、ソフトウェアの使用管理を確実にすることが出来る。

【0043】以下に、認証手順の詳細を説明する。図7は、第1の実施の形態の認証手順を示すフローチャートである。図中の破線から左側がカプセル起動プログラム311に基づくPC110の処理を表し、破線から右側がICカード200の処理を表す。

【0044】[S1] まずカプセル起動プログラム311を起動したPC110は、カプセル300の認証データをICカード200に送信する。なお、ここにいる認証データには、ユーザIDとパスワードも含まれるものとする。

【0045】ICカード200では認証データ等を用いて、以下の認証処理が行われる。

[S2] ソフトウェア認証部201aは、まずソフトウェア認証データ312に基づいてソフトウェアの認証を行う。ソフトウェアが正しいと判断されればステップS3に進み、ソフトウェアが正しくないと判断されればステップS6に進む。

【0046】[S3] ユーザ認証部201bは、ユーザがPC110に入力したユーザIDとパスワードに基づいてユーザの認証を行う。ユーザが正しいと判断されればステップS4に進み、ユーザが正しくないと判断されればステップS6に進む。

【0047】[S4] ソフトウェア使用権認証部201cは、ソフトウェア使用権認証データ313に基づいてソフトウェア使用権の認証を行う。ソフトウェアの使用権があると判断された場合にはステップS5に進み、ソフトウェアの使用権がないと判断された場合にはステップS6に進む。

【0048】なお、上記ステップS2～S4までの認証方法に関しては本発明では特に規定せず、それらは例えばRSA(Rivest Shamir Adleman) 暗号を用いた認証方法であったりDES-MAC(Message Authentication

Cord) を用いたものであったりする。

【0049】【S5】有効期限認証部201dは、有効期限認証データ314に含まれるセンタの署名314cに基づいて、有効期限開始時刻314aと有効期限終了時刻314bが正しいことを検証する。そして、ICカード200のPROM250に記憶されているICカード時刻251が有効期限終了時刻314b以下であるかどうかを確認する。有効期限認証データ314が正しいことの検証と、ICカード時刻251が有効期限終了時刻以下であることの検証の結果が正しければステップS7に進み、それらの検証の結果が正しくなければステップS6に進む。

【0050】【S6】認証部201は、ステップS2～S5の認証に失敗した場合は、PC110に対してエラーを返し、処理を終了する。

【S7】ICカード時刻更新部202は、ICカード時刻251が有効期限開始時刻314aより小さいか否かを判断し、ICカード時刻251の方が小さい場合には、ICカード時刻251を有効期限開始時刻314aで示された時刻に書き換える。

【0051】【S8】復号鍵復号部203は、暗号化された復号鍵315を、PROM250に保持されている秘密情報252を用いて復号し、PC110に返信する。

【S9】復号鍵を受け取ったPC110は、カプセル起動プログラム311の指令に基づき、暗号化されたソフトウェア320を復号し、そのソフトウェアを実行する。この時、ソフトウェア320は完全に復号されるわけではなく、実行する部分のみが復号されて揮発性メモリに展開されるようにしておき、ソフトウェアが終了されると復号され揮発性メモリに展開されたソフトウェアは消去するようにしておけば、復号されたソフトウェアが不正に使用されることはない。

【0052】このように、カプセルの有効期限を有効期限開始時刻314aと有効期限終了時刻314bとで管理し、カプセルの実行時にICカード時刻251と比較しICカード時刻251が有効期限開始時刻314aより小さい場合はICカード時刻251を有効期限開始時刻314aで更新するようにしたことにより、ユーザが新しいカプセルをセンタまたはプロバイダから入手し実行するとICカード時刻が更新され、新しいカプセルの有効期限開始時刻よりも小さい有効期限終了時刻が設定されているカプセルは使用することができなくなる。その結果、ICカードに時計を持たせなくてもソフトウェア使用権の有効期限管理を行うことが可能である。

【0053】例えば、1997年7月1から1ヶ月間の有効期限（有効期限開始時刻：1997年7月1日、有効期限終了時刻：1997年7月31日）が設定されたカプセルを実行すると、ICカード時刻には、必ず1997年7月1以降の時刻が設定される。すると、その後

は、有効期限終了時刻が1997年6月30日以前であるカプセルを実行することは出来ない。

【0054】以下に、本発明に関連する技術を、他の実施の形態として説明する。なお、図2～図5に示した構成は後述する他の実施の形態においても同様であるため、各実施の形態の説明においても図2～図5に示した符号を用いて説明する。ただし、ICカードの処理機能に関しては、個別の符号を付して説明するものとする。

【0055】まず、第2の実施の形態について説明する。この実施の形態は、ICカードの時刻の更新をPCからの時刻設定コマンドによって行うものである。図8は、第2の実施の形態におけるICカードの処理機能を示すブロック図である。本実施の形態のICカード400の処理機能の中で、認証部401中のソフトウェア認証部401a、ユーザ認証部401b及びソフトウェア使用権認証部401cと、復号鍵復号部403との有する機能は、図6に示した第1の実施の形態における同名の構成要素と同じであるため、説明を省略する。すなわち、本実施の形態は、有効期限認証部401dとICカード時刻更新部402との処理機能が、第1の実施の形態と異なる。また、第1の実施の形態と同様に、ICカード400内には、ICカード時刻451と秘密情報452とが保持されている。

【0056】PC110は、ユーザからの入力に応じて、若しくは所定のタイミングで時刻設定処理を行う。時刻設定処理では、PC110内部の時計時刻を時刻設定コマンドに含めて、ICカード400に送る。

【0057】ICカード時刻更新部402は、PC110から時刻設定コマンドを受け取ると、ICカード時刻451の更新を行い、更新ステータス（「正常終了」又は「エラー」）をPC110に返す。

【0058】図9は、時刻設定コマンドが発行された際の処理手順を示すフローチャートである。この図において破線から左側をPC110、破線から右側をICカード400とする。

【0059】【S11】PC110によって発行された時刻設定コマンドにより、PC時刻（PC110内の時計の時刻）がICカード400のICカード時刻更新部402に渡される。

【0060】【S12】PC時刻を受け取ったICカード時刻更新部402は、PC時刻とICカード時刻451とを比較し、「PC時刻>ICカード時刻」であった場合はステップS14に進み、「PC時刻>ICカード時刻」が成り立たなかった場合はステップS13に進む。

【0061】【S13】ICカード時刻更新部402は、「PC時刻>ICカード時刻」が成り立たなかった場合、すなわち現在のICカード時刻451よりも小さな値で時刻を更新しようとした場合は、PC110にエラーステータスを返し、処理を終了する。

【0062】[S14] ICカード時刻更新部402は、「PC時刻>ICカード時刻」であった場合、ICカード時刻451をPC時刻で更新し、PC110に正常終了のステータスを返す。

【0063】このように時刻設定コマンドでは、ICカードの時刻を進める方には更新できるが、時刻を戻す方には更新できないようになっている。図10は、第2の実施の形態の認証手順を示すフローチャートである。この図において破線から左側がカプセル起動プログラムに基づいて処理を実行するPC110を表し、破線から右側がICカード400を表す。

【0064】[S21] PC110においてカプセル起動プログラム311が起動されると、カプセルの認証データがICカード400へ送信される。ICカード400では認証データ等を用いて、以下の認証処理が行われる。

【0065】[S22] ソフトウェア認証部401aは、ソフトウェア認証データ312に基づいてソフトウェアの認証を行う。ソフトウェアが正しいと判断されればステップS23に進み、ソフトウェアが正しくないと判断されればステップS26に進む。

【0066】[S23] ユーザ認証部401bは、ユーザがPC110に入力したユーザIDとパスワードに基づいてユーザの認証を行う。ユーザが正しいと判断されればステップS24に進み、ユーザが正しくないと判断されればステップS26に進む。

【0067】[S24] ソフトウェア使用権認証部401cは、ソフトウェア使用権認証データ313に基づいてソフトウェア使用権の認証を行う。ソフトウェアの使用権があると判断された場合にはステップS25に進み、ソフトウェアの使用権がないと判断された場合にはステップS26に進む。

【0068】[S25] 有効期限認証部401dは、有効期限認証データ314に含まれるセンタの署名314cに基づいて、有効期限開始時刻314aと有効期限終了時刻314bが正しいことを検証する。そして、ICカード400に記憶されているICカード時刻451が有効期限開始時刻314a以上であり、かつ有効期限終了時刻314b以下であるかどうかを確認する。有効期限認証データが正しいことの検証と、ICカード時刻451が有効期限内であることの検証の結果が正しければステップS27に進み、それらの検証の結果が正しくなければステップS26に進む。

【0069】[S26] 認証部401は、ステップS22～S25のいずれかの認証に失敗した場合はPC110に対してエラーを返し、処理を終了する。

[S27] 復号鍵復号部403は、暗号化された復号鍵315を、秘密情報452を用いて復号し、PC110に返信する。

【0070】[S28] 復号鍵を受け取ったPC110

は、カプセル起動プログラム311の指令に基づき、その復号鍵を用い暗号化されたソフトウェア320を復号し、そのソフトウェアを実行する。

【0071】以上のような処理機能を有するPC110とICカード400を用い、ユーザが、まず第1のカプセルを実行し、次に第2のカプセルを実行する場合を想定し、本実施の形態の処理手順を具体的に説明する。

【0072】図11は、カプセルの有効期限とICカード時刻の変化とを示す図である。第1のカプセルの有効期限41は、1997年7月1日から1997年7月31日までであり、第2のカプセルの有効期限42は、1997年9月1日から1997年9月30日までである。なお、現在の正しい時刻は「1997年9月15日」であるが、ユーザは、PCの時刻をごまかしてソフトウェアを利用しているものとする。また、カプセルを実行前のICカード時刻には、1997年7月1日以前の時刻51が設定されているものとする。

【0073】ここで、ユーザが第1のカプセルを実行する場合には、時刻51に設定されているICカード時刻451を、第1のカプセルの有効期限41内の時刻に更新しなければならない。そこでユーザは、PC時刻を「1997年7月15日」に設定する。そして、PC110から時刻設定コマンドが発行されると、その時刻52がICカード時刻451として設定される。これにより、ユーザは不正に第1のカプセルを実行できる。

【0074】次に、ユーザが新しい第2のカプセルを入手して実行する場合には、時刻52に設定されているICカード時刻451を、第2のカプセルの有効期限42内の時刻に更新しなければならない。そこでユーザは、PC時刻を正しい時刻「1997年9月15日」に設定し、PC110から時刻設定コマンドを発行する。すると、その時刻53がICカード時刻451になる。これにより、ユーザは第2のカプセルを正当に実行できる。

【0075】その後、ユーザが第1のカプセルを実行しようとしてもICカード時刻451には、時刻53が設定されており第1のカプセルの有効期限41の範囲外となっているので、再び第1のカプセルを使用することは出来なくなる。また、ICカード時刻451は、時刻を増加させることのみが可能であるため、ICカード時刻451を第1のカプセルの有効期限41の範囲内に戻すことは出来ない。

【0076】このようにカプセルの有効期限を有効期限開始時刻と有効期限終了時刻とで管理し、カプセルの実行時にICカード時刻と比較しICカード時刻が有効期限内でないと実行できないようにしてあるので、ユーザが新しいカプセルをセンタまたはプロバイダから入手し実行しようとするICカード時刻を更新しなければならない。そのため、新しいカプセルの有効期限開始時刻よりも小さい有効期限終了時刻が設定されているカプセルは使用することができなくなり、ICカードに時計を

持たせなくてもソフトウェア使用权の有効期限管理を行うことが可能である。

【0077】次に、第3の実施の形態について説明する。この実施の形態は、使用期限の管理に加えて利用回数の管理を行うことにより、より確実に不正使用の防止を図ったものである。

【0078】図12は、第3の実施の形態におけるICカードの処理機能を示すブロック図である。本実施の形態のICカード500の処理機能の中で、ソフトウェア認証部501a、ユーザ認証部501b、ソフトウェア使用权認証部501c、有効期限認証部501d及び復号鍵復号部503の有する機能は、図8に示した第2の実施の形態における同名の構成要素と同じであるため、説明を省略する。

【0079】利用回数カウンタ504は、ICカード500がユーザに渡される際に、プロバイダ若しくはセンタ130によって所定の値が初期値として設定されており、認証部501により使用が許可される度に、設定されている値を1だけ減算する。

【0080】認証部501内に設けられた利用回数制限認証部501eは、利用回数カウンタ504の値が0であればソフトウェアの使用を許可し、0以外の値であればソフトウェアの使用を認める。

【0081】乱数生成部505は、PC110からチャレンジ要求を受け取ると、乱数を生成する。乱数暗号化部506は、乱数生成部505が生成し乱数を秘密鍵を用いて暗号化し、チャレンジとしてPC110へ転送する。

【0082】レスポンス検証部507は、PC110からのレスポンスをセンタの公開鍵で復号し、レスポンスに含まれる乱数と乱数生成部505で生成した乱数とが一致するか否かに基づき、レスポンスが正しいことを検証する。レスポンスが正しくない場合には、PC110にエラーを返す。レスポンスが正しいければ、その旨の情報を、ICカード時刻更新部502とカウンタ初期化部508とに伝える。その際、センタ時刻の情報をICカード時刻更新部502へ渡す。

【0083】ICカード時刻更新部502は、レスポンス検証部507からレスポンスが正しい旨の情報を受け取ると、センタ時刻がICカード時刻より大きい場合には、レスポンス検証部507から送られたセンタ時刻で、ICカード時刻551を更新する。

【0084】カウンタ初期化部508は、レスポンス検証部507からレスポンスが正しい旨の情報を受け取ると、利用回数カウンタ504を初期化する。このような機能を有するICカード500を用い、以下のような認証処理を行う。

【0085】図13は、第3の実施の形態の認証手順を示すフローチャートである。この図において破線から左側がカプセル起動プログラムに基づいて処理を実行する

PC110を表し、破線から右側がICカード500を表す。

【0086】【S31】PC110においてカプセル起動プログラム311が起動されると、カプセルの認証データがICカード500へ送信される。ICカード500では認証データ等を用いて、以下の認証処理が行われる。

【0087】【S32】ソフトウェア認証部501aは、ソフトウェア認証データ312に基づいてソフトウェアの認証を行う。ソフトウェアが正しいと判断されればステップS33に進み、ソフトウェアが正しくないと判断されればステップS37に進む。

【0088】【S33】ユーザ認証部501bは、ユーザがPC110に入力したユーザIDとパスワードに基づいてユーザの認証を行う。ユーザが正しいと判断されればステップS34に進み、ユーザが正しくないと判断されればステップS37に進む。

【0089】【S34】ソフトウェア使用权認証部501cは、ソフトウェア使用权認証データ313に基づいてソフトウェア使用权の認証を行う。ソフトウェアの使用权があると判断された場合にはステップS35に進み、ソフトウェアの使用权がないと判断された場合にはステップS37に進む。

【0090】【S35】有効期限認証部501dは、有効期限認証データ314に含まれるセンタの署名314cに基づいて、有効期限開始時刻314aと有効期限終了時刻314bが正しいことを検証する。そして、ICカード500に記憶されているICカード時刻551が有効期限開始時刻314a以上であり、かつ有効期限終了時刻314b以下であるかどうかを確認する。有効期限認証データが正しいことの検証と、ICカード時刻551が有効期限内であることの検証の結果が正しいければステップS36に進み、それらの検証の結果が正しくなければステップS37に進む。

【0091】【S36】利用回数制限認証部501aは、利用回数カウンタが0でないことを確かめ、利用回数カウンタが0であればステップS37に進み、利用回数カウンタが0でない場合にはステップS38に進む。

【0092】【S37】認証部501は、ステップS32～S36のいずれかの認証に失敗した場合はPC110に対してエラーを返し、処理を終了する。

【S38】利用回数カウンタ504は、認証部501から使用を許可する旨の信号が出力されると、設定されている値を1だけ減算する。

【0093】【S39】暗号化された復号鍵をICカード500の秘密情報552を用いて復号しPC110に返信する。

【S40】PC110は、カプセル起動プログラム311の命令に従い、返信された復号鍵を用い暗号化されたソフトウェア320を復号しソフトウェアを実行する。

【0094】なお、以上の説明では利用回数カウンタ504がある値から減算され0になるとカプセルを実行できないようにしているが、逆に利用回数カウンタを0からスタートさせ、ある値になるとカプセルを実行できないようにしてもよい。

【0095】上記の説明で利用回数カウンタが0となりカプセルを実行できなくなったICカードは、以下に示す操作により再びカプセルを実行できるようにすることが出来る。

【0096】図14は、利用回数カウンタのリセット処理の手順を示すフローチャートである。この図において、破線から左側はPC110、破線から右側はICカード500を表す。

【0097】[S41] PC110は、ICカード500へチャレンジ要求を出す。

[S42] ICカード500がチャレンジ要求を受け取ると、乱数生成部505が乱数rを生成する。

【0098】[S43] 乱数暗号化部506が、乱数rを公開鍵暗号方式に対応したICカード500の秘密鍵で暗号化し、それをチャレンジとしてPC110に返信する。

[S44] PC110はICカード500からチャレンジを受け取ると、そのチャレンジをセンタ130に送信し、センタ130からレスポンスを得る。レスポンスの構造としては、例えばICカードから受け取った乱数とセンタ時刻とを連結し公開鍵暗号方式に対応したセンタ130の秘密鍵で署名した構造となっている。

【0099】[S45] PC110は、センタ130から受け取ったレスポンスをICカード500へ送信する。

[S46] レスポンス検証部507はレスポンスの検証を行う。レスポンス検証の手順としてはあらかじめICカード500に登録されている公開鍵暗号方式に対応したセンタ130の公開鍵で署名の検証をし、乱数生成部505が生成した乱数rとレスポンス中のrが一致することを確認する。レスポンスの検証に成功した場合にはステップS48に進み、検証に失敗した場合にはステップS47へ進む。

【0100】[S47] レスポンスの検証に失敗した場合には、レスポンス検証部507がPC110に対してエラーを返し、処理を終了する。

[S48] センタ時刻がICカード時刻より大きい場合は、ICカード時刻更新部502が、レスポンスに含まれるセンタ時刻をICカード時刻551に代入する。

【0101】[S49] また、カウンタ初期化部508が、利用回数カウンタ504を初期値に戻し再びカプセルが使用できるようにする。

[S50] レスポンス検証部507がPC110に対して、正常終了のステータスを返す。

【0102】このようにカプセルの使用を回数で制限

し、利用回数制限に達したらカプセルを利用できなくなり、その後センタと通信しセンタの時刻でICカード時刻を更新した場合にのみ、再びカプセルを使用可能とすることで、ICカードの時刻を管理することが可能になる。

【0103】なお、上記の説明で乱数を暗号化する場合、レスポンスを検証する際に公開鍵暗号方式を例にとって説明したが、これは本発明を何ら限定するものではなくICカード500とセンタ130とにおけるデータ交換の正当性を保証できるものであれば代用可能である。また、乱数rを検証データとして用いたが、これは必ずしも乱数である必要はなくチャレンジ要求に対して毎回値が更新されるものであればよい。

【0104】また、レスポンスに利用回数の更新値を持たせることで、利用回数カウンタを任意の値だけ更新できるようにすることも可能である。次に、第4の実施の形態について説明する。この実施の形態は、センタからのICカードへのデータにセンタ時刻を含め、そのセンタ時刻によりICカード時刻を更新するものである。

【0105】図15は、第4の実施の形態におけるICカードの処理機能を示すブロック図である。本実施の形態のICカード600の処理機能の中で、認証部601（ソフトウェア認証部601a、ユーザ認証部601b、ソフトウェア使用権認証部601c及び有効期限認証部601dを含む）と復号鍵復号部603との有する機能は、図6に示した第1の実施の形態における同名の構成要素と同じであるため、説明を省略する。また、第1の実施の形態と同様に、ICカード600内には、ICカード時刻651と秘密情報652とが保持されている。

【0106】センタ署名検証部604は、センタからのデータをPC110を介して受け取ると、そのセンタの署名を検証する。正しければ、その旨をICカード時刻更新部602に通知する。また、センタの署名が正しくなければ「エラー」の更新ステータスをPC110に返す。

【0107】ICカード時刻更新部602は、ICカード時刻651とセンタ時刻とを比較し、センタ時刻の方が大きければ、ICカード時刻651をセンタ時刻に更新する。

【0108】図16は、センタからのデータの例を示す図である。センタからのデータ60は、ICカード600に発行するデータ61、センタからのデータ60が発行されたときのセンタ時刻62、およびデータ61とセンタ時刻62に対するセンタの署名63で構成される。ここでセンタからのデータとは、センタから発行された任意のデータを指し、例えばカプセルそのものであったり、何かのサービスを取得するためのチケットのようなものであったり、ただ単にセンタからのメッセージだったりする。

【0109】図17は、第4の実施の形態におけるICカード時刻の更新手順を示すフローチャートである。この図において破線から左側がPC110を表し、破線から右側がICカード600を表す。

【0110】【S61】PC110はICカード600にセンタ130からのデータ60を送信する。

【S62】センタ署名検証部604は、センタ130からのデータ60を受け取ると、センタの署名の検証を行いICカード600に発行するデータ61とセンタ時刻62が正当であることを検証する。検証に成功した場合は、データ60に応じた処理を行った後、ステップS64へ進む。検証に失敗した場合は、ステップS63に進む。

【0111】【S63】センタ署名検証部604は、PC110に対してエラーを返し、処理を終了する。

【S64】ICカード時刻更新部602は、センタ時刻62とICカード時刻651とを比較する。センタ時刻62がICカード時刻651より大きい場合にはステップS65に進み、それ以外の場合にはステップS66に進む。

【0112】【S65】ICカード時刻更新部602は、センタ時刻62をICカード時刻651に代入する。

【S66】ICカード時刻更新部602は、PC110に対し、正常終了の更新ステータスを返す。

【0113】このようにセンタからICカードに発行されるデータにはセンタ時刻とセンタの署名をつけるようにすることで、ICカードの時刻管理を可能とすることが出来る。

【0114】なお、上記のICカードの有する機能の処理内容は、ROMに格納された認証プログラムをICカード内のCPUが実行することで実現されているが、この認証プログラムを他の記録媒体に格納しておくこともできる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場を流通させる場合には、CD-ROMやフロッピー（登録商標）ディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【0115】

【発明の効果】以上説明したように本発明のサービス提供システムでは、サービスの有効期限を有効期限開始時刻と有効期限終了時刻とで管理し、認証装置の認証用時刻を有効期限開始時刻を用いて更新するようにしたため、ローカルなサービス提供装置であっても、内部に時計を持たない認証装置を用いてサービスの利用権の有効

期限の管理を行うことが可能となる。

【0116】また、本発明の認証装置では、サービス提供装置からの要求に応じて有効期限の認証を行うと共に、認証用時刻を有効期限開始時刻を用いて更新するようにしたため、内部に時計を持たずに、有効期限の認証を行うことが可能となる。

【0117】また、本発明の認証プログラムを記録したコンピュータ読み取り可能な記録媒体では、サービス提供装置からの要求に応じて有効期限の認証を行うと共に、認証用時刻を有効期限開始時刻を用いて更新するようなプログラムを格納したため、格納したプログラムをコンピュータで実行させれば、内部時計を用いない有効期限の認証をコンピュータに行わせることが可能となる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】ICカードを用いた認証システムの概略構成を示す図である。

【図3】カプセルの例を示す図である。

【図4】有効期限認証データの構造を示す図である。

【図5】ICカードのハードウェア構成を示す図である。

【図6】ICカードの処理機能を示すブロック図である。

【図7】第1の実施の形態の認証手順を示すフローチャートである。

【図8】第2の実施の形態におけるICカードの処理機能を示すブロック図である。

【図9】時刻設定コマンドが発行された際の処理手順を示すフローチャートである。

【図10】第2の実施の形態の認証手順を示すフローチャートである。

【図11】カプセルの有効期限とICカード時刻の変化とを示す図である。

【図12】第3の実施の形態におけるICカードの処理機能を示すブロック図である。

【図13】第3の実施の形態の認証手順を示すフローチャートである。

【図14】利用回数カウンタのリセット処理の手順を示すフローチャートである。

【図15】第4の実施の形態におけるICカードの処理機能を示すブロック図である。

【図16】センタからのデータの例を示す図である。

【図17】第4の実施の形態におけるICカード時刻の更新手順を示すフローチャートである。

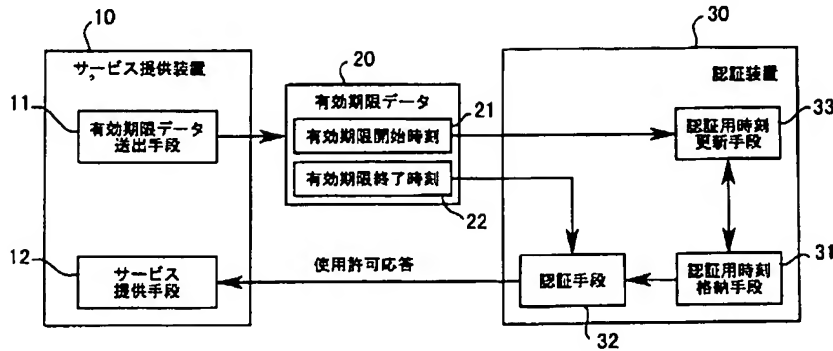
【符号の説明】

- 10 サービス提供装置
- 11 有効期限データ送出手段
- 12 サービス提供手段
- 20 有効期限データ

- 21 有効期限開始時刻  
22 有効期限終了時刻  
30 認証装置

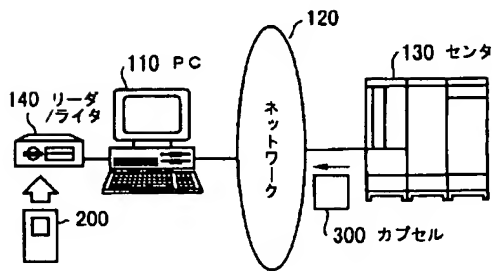
- 31 認証用時刻格納手段  
32 認証手段  
33 認証用時刻更新手段

【図1】

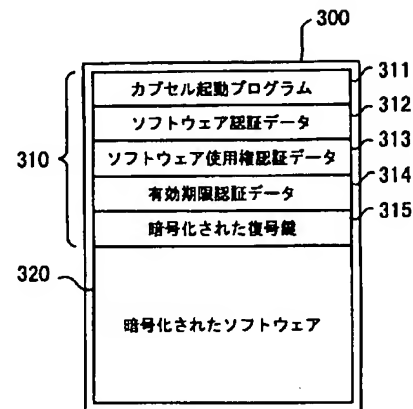


【図2】

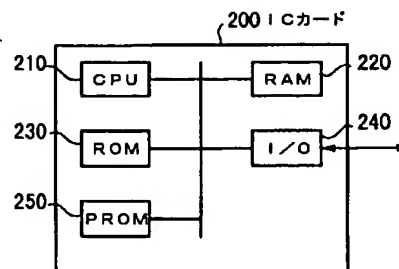
【図3】



【図4】

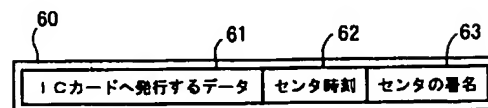
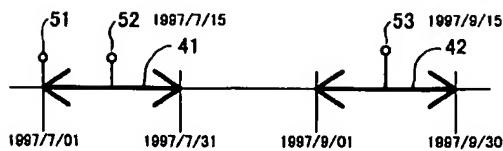


【図5】

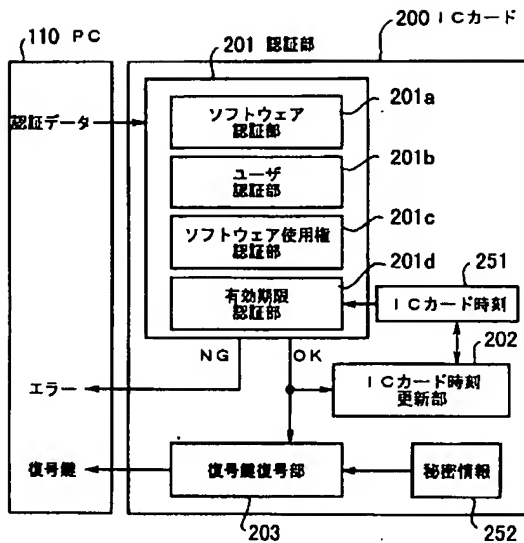


【図11】

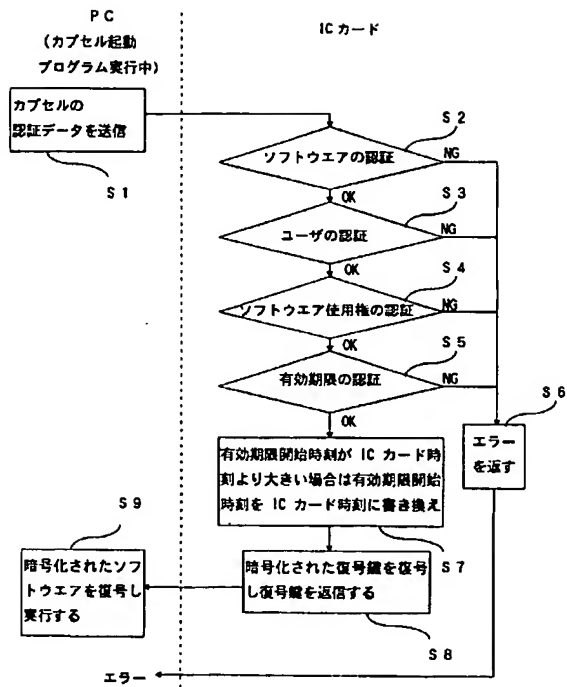
【図16】



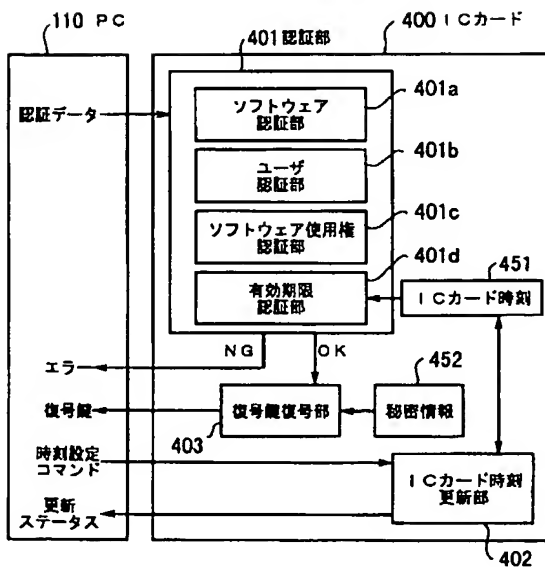
【図6】



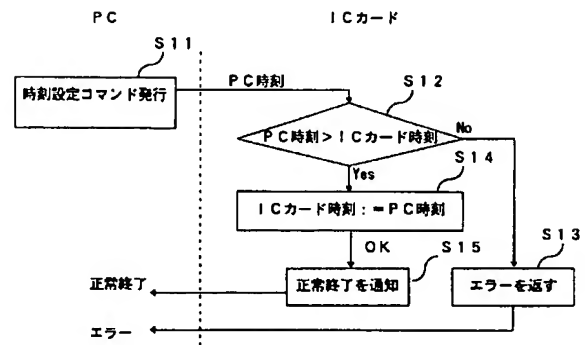
【図7】



【図8】

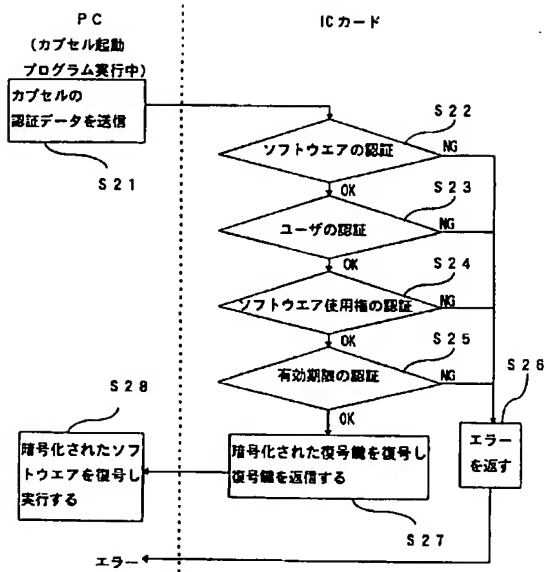


【図9】

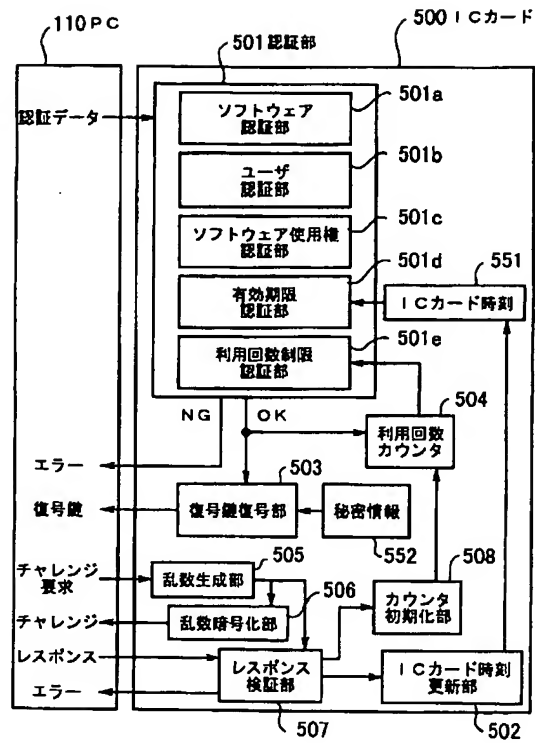




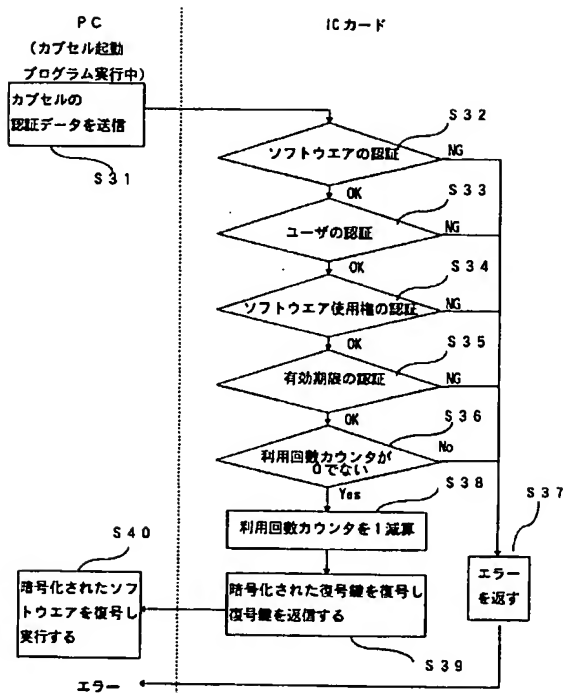
【図10】



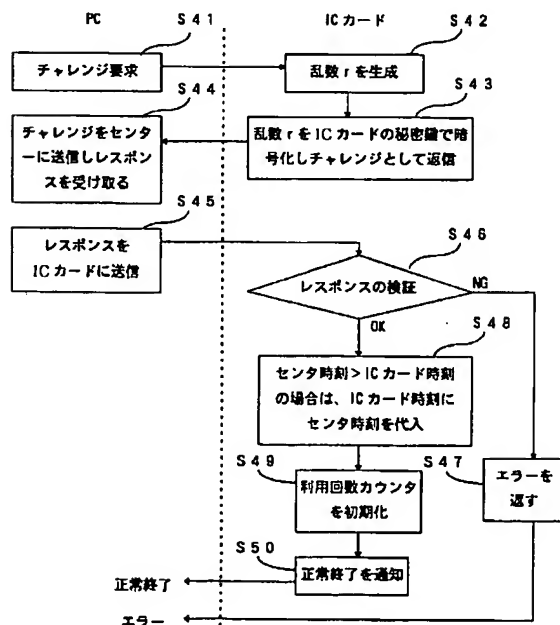
【図12】



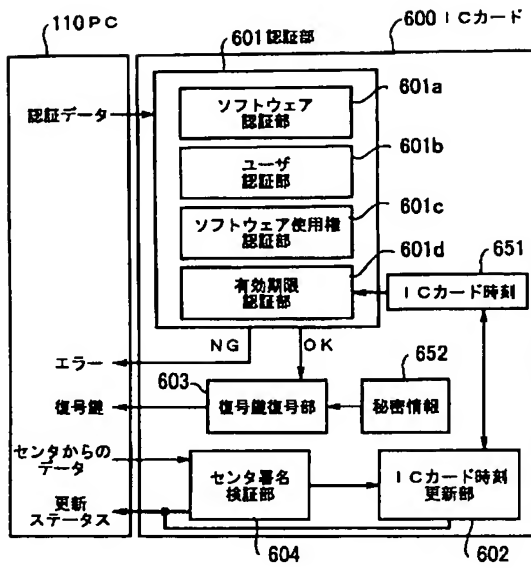
【図13】



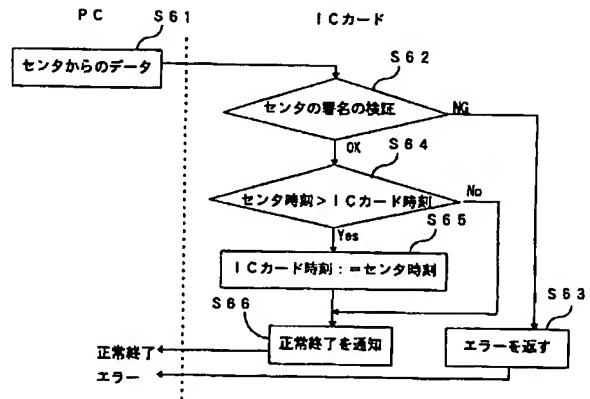
【図14】



【図15】



【図17】



フロントページの続き

(72)発明者 千葉 健司  
 神奈川県足柄上郡中井町境430 グリーン  
 テクナイク 富士ゼロックス株式会社内

Fターム(参考) 5B085 AE02 AE03 AE06 AE12  
 5J104 AA07 AA11 MA01 PA10